English Translation of Relevant Portions of JP-A-H11-265349
Published on September 28, 1999

:

:

Page (8), column 13, lines 39 – 47

[0052] For example, in Fig. 4, the key that a user AAAA currently uses for encryption/decryption is the key (B). An acceptable error range of the expiration date is set with the difference between the times shown by the clocks of the systems taken into consideration. In the case where decryption cannot be achieved with the current key and the acceptable error range has not expired, decryption is tried again with a key whose generation management number is 0. Likewise, in the case where, after the key change, decryption cannot be achieved with the current key and the acceptable error range has not expired, decryption is tried again using a key whose generation management number is 2.

:

:

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-265349
(43)Date of publication of application : 28.09.1999

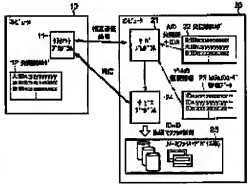
(51)Int.Cl. G06F 15/00
G09C 1/00
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 10-066670
(22)Date of filing : 17.03.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : OOYAMA MASAKO

(54) COMPUTER SYSTEM AND SECRET PROTECTION METHOD, TRANSMITTING/RECEIVING LOG MANAGEMENT METHOD, MUTUAL CHECKING METHOD, AND A DISCLOSED KEY GENERATION MANAGEMENT METHOD TO BE APPLIED TO ITS SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a computer system capable of easily integrating a mutual certification function while applying access control matched with the security policy of an existing system.
SOLUTION: At the time of receiving a certification request from a client program 11, a server program 21 checks the identity of the opposite party by a challenge and response system by using a disclosed key stored in a disclosed key holder 22. When the certification succeeds, the program 21 extracts an identifier(ID) allowed to correspond to the disclosed key from the holder 22 and extracts user management data for the program 11 from a user management data file 23 based on the ID. In the case of starting an optional service program 24 requested from the program 11, a right range indicated by the extracted user management data is applied to the program 24.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平11－265349

(43)公開日　平成11年(1999) 9月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
G06F 15/00	330	G06F 15/00	330D
G09C 1/00	630	G09C 1/00	630F
	640		640B
H04L 9/08		H04L 9/00	601F
9/32			675B

審査請求　未請求　請求項の数27　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－68670

(22)出願日　平成10年(1998) 3月17日

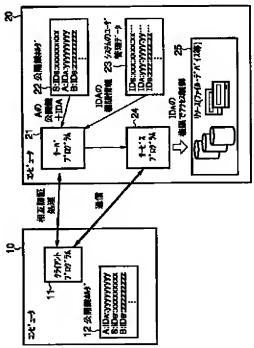
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　大山　真砂子
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　コンピュータシステムならびに同システムに適用される機密保護方法、送受信ログ管理方法、相互の確認方法および公開鍵世代管理方法

(57)【要約】
【課題】既存のシステムのセキュリティ・ポリシーに沿ったアクセス制御を適用しつつ相互認証機能を容易に組み込むことのできるコンピュータシステム。
【解決方法】サーバプログラム２１は、クライアントプログラム１１からの認証要求を受けた際、公開鍵ホルダ２２に格納された公開鍵を用いてチャレンジ＆レスポンス方式により相手の身元確認を行なう。この認証が成立すると、サーバプログラム２１は、その公開鍵に対応づけられた識別子を公開鍵ホルダ２２から取り出し、その識別子をもとにクライアントプログラム１１のユーザ管理データをユーザ管理データファイル２３から取り出す。そして、クライアントプログラム１１が要求した任意のサービスプログラム２４を起動する際、その取り出したユーザ管理データで示される権限範囲をそのサービスプログラム２４に与える。



1

【特許請求の範囲】

【請求項１】　公開鍵暗号を用いたワンタイムパスワード方式の相互認証を実行する相互認証機能および前記相互認証を実行し合う相手からの要求に応じてプログラムを起動するサービス機能を有するコンピュータシステムにおいて、前記相手に与える自システム内での権限を決定する識別子を前記相互認証に供される公開鍵と対応づけて格納する識別子格納手段と、

前記相互認証の成立を条件に起動される前記相手から要求されたプログラムに対して、その相互認証に供された公開鍵と対応づけられた前記識別子で決定される権限を与える権限付与手段とを具備することを特徴とするコンピュータシステム。

【請求項２】　前記識別子格納手段は、前記識別子を前記公開鍵が格納される公開鍵ホルダ内で前記公開鍵と対にして格納することを特徴とする請求項１記載のコンピュータシステム。

【請求項３】　前記識別子格納手段は、前記識別子と前記公開鍵とを対応づけるマッピングテーブルを備えることを特徴とする請求項１記載のコンピュータシステム。

【請求項４】　前記自システム内での権限を含む前記他のコンピュータに関するユーザ管理データを前記識別子と対応づけて管理するユーザ管理データ格納手段をさらに具備し、

前記権限付与手段は、前記相互認証に供された公開鍵と対応づけられた識別子から前記ユーザ管理データを得て、その得られたユーザ管理データで示される権限を前記起動されるプログラムに付与する手段を有することを特徴とする請求項１、２または３記載のコンピュータシステム。

【請求項５】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、

送信側および受信側のコンピュータ双方に、

前記データ授受の事実を証明するためのログを格納するログファイルと、

前記転送データの授受が成立したときに、相手方の電子署名、日時、相手を識別するための識別情報および転送データを識別するための識別情報を含むログを採取して前記ログファイルに記録するログ採取手段とを設けたことを特徴とするコンピュータシステム。

【請求項６】　送信側および受信側のコンピュータ双方に、前記転送データを検証用に退避しておく転送データ退避手段をさらに設けたことを特徴とする請求項５記載のコンピュータシステム。

【請求項７】　前記ログ採取手段は、前記ログファイルにログを記録した後に前記転送データの授受が無効化されたときに、前記ログファイルから前記記録したログを削除する手段を有することを特徴とする請求項５記載のコンピュータシステム。

2

【請求項８】　データの転送中にエラーが発生した場合に、受信側コンピュータにおいて受信したデータを破棄する手段をさらに具備したことを特徴とする請求項５記載のコンピュータシステム。

【請求項９】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、

受信側のコンピュータに、

前記転送データを正規に受け入れるときに、その旨を伝えるための受信通知として前記転送データを一意に識別可能な情報を元に生成した電子署名を返送する受信通知手段を設けたことを特徴とするコンピュータシステム。

【請求項１０】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、

送信側のコンピュータに、

前記転送データとその時点でのシステム日時とから電子署名を生成する電子署名生成手段と、

前記転送データに前記システム日付および前記電子署名生成手段により生成された電子署名を付加して送信する送信手段とを設け、

受信側のコンピュータに、

前記転送データを前記システム日付を付加した状態で前記電子署名により検証する検証手段を設けたことを特徴とするコンピュータシステム。

【請求項１１】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、

受信側のコンピュータに、

前記転送データを正規に受け入れるときに、その旨を伝えるための受信通知として前記転送データを一意に識別可能な情報とその時点でのシステム日時とを元に生成した電子署名および前記システム日付を返送する受信通知手段を設け、

送信側のコンピュータに、

前記電子署名を前記システム日付を付加した状態で検証する検証手段を設けたことを特徴とするコンピュータシステム。

【請求項１２】　第１のコンピュータと第２のコンピュータとの間で公開鍵暗号方式を用いたデータ処理を行なうコンピュータシステムにおいて、

前記第１および第２のコンピュータ双方に、

それぞれに有効期間が設定された同一人を認証するための複数の公開鍵を前記有効期間に基づいて世代管理する公開鍵世代管理手段を設けたことを特徴とするコンピュータシステム。

【請求項１３】　前記公開鍵世代管理手段は、未使用、使用中および使用済みのいずれかを示す状態フラグを前記世代管理する複数の公開鍵それぞれに対応させて管理する手段を有することを特徴とする請求項１２記載のコ

ンピュータシステム。

【請求項14】　前記公開鍵世代管理手段は、前記世代管理する複数の公開鍵が使用された順番を管理する手段を有することを特徴とする請求項12記載のコンピュータシステム。

【請求項15】　他方のコンピュータから要求された認証が不成立であったときに、前記公開鍵世代管理手段により管理された未使用あるいは使用済みの公開鍵であってその有効期間と自己のシステム日付との差が予め定められた許容範囲内にある公開鍵を取り出し、その取り出した公開鍵を用いて前記認証を再試行させる認証再試行手段をさらに具備することを特徴とする請求項12記載のコンピュータシステム。

【請求項16】　公開鍵暗号を用いたワンタイムパスワード方式の相互認証を実行する相互認証機能および前記相互認証を実行し合う相手からの要求に応じてプログラムを起動するサービス機能を有するコンピュータシステムの機密保護方法であって、

前記相手に与える自システム内での権限を決定する識別子を前記相互認証に供される公開鍵と対応づけて格納するステップと、

前記相互認証の成立を条件に起動される前記相手から要求されたプログラムに対して、その相互認証に供された公開鍵と対応づけられた前記識別子で決定される権限を与えるステップとを具備することを特徴とする機密保護方法。

【請求項17】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行し、前記データ授受の事実を証明するためのログを格納するログファイルを有するコンピュータシステムの送受信ログ管理方法であって、

前記転送データの授受が成立したときに、相手方の電子署名、日時、相手を識別するための識別情報および転送データを識別するための識別情報を含むログを採取して前記ログファイルに記録するステップを具備することを特徴とする送受信ログ管理方法。

【請求項18】　前記ログファイルにログを記録した後に前記転送データの授受が無効化されたときに、前記ログファイルから前記記録したログを削除するステップをさらに具備することを特徴とする請求項16記載の送受信ログ管理方法。

【請求項19】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおける相互の確認方法であって、

送信側のコンピュータは、

前記転送データとその時点でのシステム日時とから電子署名を生成するステップと、

前記転送データに前記システム日付および前記電子署名生成手段により生成された電子署名を付加して送信するステップとを具備し、

受信側のコンピュータ側は、

前記転送データを正規に受け入れるときに、その旨を伝えるための受信通知として前記送信側のシステム日付および電子署名が付加された転送データを一意に識別可能な情報とその時点でのシステム日時とを元に生成した電子署名および前記システム日付を返送するステップを具備することを特徴とする相互の確認方法。

【請求項20】　第1のコンピュータと第2のコンピュータとの間で公開鍵暗号方式を用いたデータ処理を行なうコンピュータシステムにおける公開鍵世代管理方法であって、

それぞれに有効期間が設定された同一人を認証するための複数の公開鍵を前記有効期間に基づいて世代管理するステップを具備することを特徴とする公開鍵世代管理方法。

【請求項21】　他方のコンピュータから要求された認証が不成立であったときに、前記管理された未使用あるいは使用済みの公開鍵であってその有効期間と自己のシステム日付との差が予め定められた許容範囲内にある公開鍵を取り出し、その取り出した公開鍵を用いて前記認証を再試行させるステップをさらに具備することを特徴とする請求項20記載の公開鍵世代管理方法。

【請求項22】　公開鍵暗号を用いたワンタイムパスワード方式の相互認証を実行する相互認証機能および前記相互認証を実行し合う相手からの要求に応じてプログラムを起動するサービス機能を有するコンピュータシステムの機密保護を制御するためのプログラムであって、

前記相手に与える自システム内での権限を決定する識別子を前記相互認証に供される公開鍵と対応づけて格納し、

前記相互認証の成立を条件に起動される前記相手から要求されたプログラムに対して、その相互認証に供された公開鍵と対応づけられた前記識別子で決定される権限を与えるように前記コンピュータシステムを動作させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項23】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行し、前記データ授受の事実を証明するためのログを格納するログファイルを有するコンピュータシステムの送受信ログ管理を制御するためのプログラムであって、

前記転送データの授受が成立したときに、相手方の電子署名、日時、相手を識別するための識別情報および転送データを識別するための識別情報を含むログを採取して前記ログファイルに記録するように前記コンピュータシステムを動作させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項24】　前記プログラムは、さらに前記ログファイルにログを記録した後に前記転送データの授受が無

効化されたときに、前記ログファイルから前記記録したログを削除するように前記コンピュータシステムを動作させる請求項２３記載の記録媒体。

【請求項２５】　転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおける相互の確認を制御するためのプログラムであって、

送信側のコンピュータを、

前記転送データとその時点でのシステム日時とから電子署名を生成し、

前記転送データに前記システム日付および前記電子署名生成手段により生成された電子署名を付加して送信するように動作させ、

受信側のコンピュータを、

前記転送データを正規に受け入れるときに、その旨を伝えるための受信通知として前記送信側のシステム日付および電子署名が付加された転送データを一意に識別可能な情報とその時点でのシステム日時とを元に生成した電子署名および前記システム日付を返送するように動作させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２６】　第１のコンピュータと第２のコンピュータとの間で公開鍵暗号方式を用いたデータ処理を行なうコンピュータシステムにおける公開鍵世代管理を制御するためのプログラムであって、

それぞれに有効期間が設定された同一人を認証するための複数の公開鍵を前記有効期間に基づいて世代管理するように前記コンピュータシステムを動作させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項２７】　前記プログラムは、さらに他方のコンピュータから要求された認証が不成立であったときに、前記管理された未使用あるいは使用済みの公開鍵であってその有効期間と自己のシステム日付との差が予め定められた許容範囲内にある公開鍵を取り出し、その取り出した公開鍵を用いて前記認証を再試行させるように前記コンピュータシステムを動作させる請求項２６記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータネットワークを介して接続される複数のコンピュータ相互間で相互認証を実行するコンピュータシステムならびに同システムに適用される機密保護方法、送受信ログ管理方法、相互認証方法および公開鍵世代管理方法に関する。

【０００２】

【従来の技術】近年のコンピュータ技術およびネットワーク技術の高度化に伴ない、リモートシステム間でのデータ送受信が頻繁に行なわれるようになってきた。そして、このリモートシステム間でのデータ送受信の安全性を確保するための技術として以下よりなものが存在する。

（１）公開鍵暗号を用いたチャレンジ＆レスポンス方式により認証する技術毎回、異なる乱数を生成し、その生成した乱数を公開鍵暗号により暗号化したデータをパスワードとして利用する技術である。具体的には、次のような処理を行なう。

（ａ）認証要求を受けた際に、認証する側が乱数を生成して、認証される側にこれを送信する。

（ｂ）認証される側は、これを自身の秘密鍵により暗号化して、認証する側にこれを送信する。

（ｃ）認証する側は、これを相手の公開鍵により復号化して、相手の身元を確認する。

【０００３】一般に、この公開鍵暗号を用いたチャレンジ＆レスポンス方式により認証する技術は、ネットワーク上を搬送するパスワードを保護するための方法である。毎回、使い捨てのパスワードを使用（ワンタイムパスワード方式）することによって、パスワードの盗聴や再送などによる抜害を防ぐ。そして、公開鍵暗号方式として安全性の高いＲＳＡや楕円曲線暗号を用いることで、高い安全性を保つことができる。

（２）送信データに付加した電子署名により、送信者の「なりすまし」やネットワーク上での「データの改ざん、破壊」を防ぐ技術データを送信する際に、対象データを一方向関数により要約し、これを自身の秘密鍵にて暗号化した電子署名を生成する。これを送信データに付加してネットワーク上に送り出す。

【０００４】受信側では、データ受信時に、その受信したデータを同様に一方向関数で要約した値と電子署名データを送信者の公開鍵で復号化した結果とを比較する。これにより、図６に示すように、第３者による送信者のなりすましやネットワーク上でのデータの改ざんまたは破壊などを防止する。

【０００５】

【発明が解決しようとする課題】ところで、これまでの認証技術では、認証成立後、アクセスを許可されたユーザに適用されるアクセス制御や権限範囲などが明確でなく、認証されたユーザへのアクセス制御は、各アプリケーションにまかされていた。この結果、以下のような問題が発生する。

（１）アプリケーションごとに異なるセキュリティーポリシーが適用され、システムの一貫性が失われてしまう虞があり、それに起因してシステムの安全性を低下させてしまう虞がある。

（２）管理者の負荷が重くなってしまう。

（３）安全性の検査やアプリケーションの開発が困難となる。

【０００６】また、これまでの安全性を重視したデータ転送機能においては、暗号化や電子署名といった技術により、データの漏洩や改ざんなどの脅威を払拭すること

は可能であるが、送信者は、正しい相手に正しいデータが受信されていることを確認する術がなかった。また、データ転送の後に、送信者または受信者がデータの授受を否定したときに、それを解析することはできても、決定的に証明する方法がなかった。このために、送受信者の利害が絡んだデータを転送したときに、データ受信否認などのトラブルが発生したとしても、それを解決する手段がないといった問題があった。

【0007】さらに、これまでは、暗号鍵を使い捨てで利用してきたが、前述したような検証を再現するような場合には、そのデータ転送時に使用されていた鍵が必要となる。また、鍵を更新する場合に、正しくデータ転送が行なわれるためには、送信側および受信側の双方で、使用する秘密鍵と公開鍵との組を必ず同じ時点で更新されていなければならない。しかしながら、現在では、鍵の登録は人手を介して行なわれているケースがほとんどであるために、リモートのシステム上で、この鍵更新の同期をとる処理は非常に困難であった。

【0008】この発明はこのような実情に鑑みてなされたものであり、たとえば既存のシステムのセキュリティ・ポリシーに沿ったアクセス制御を適用しつつ、相互認証機能を容易に組み込むことのできるコンピュータシステムおよび同システムに適用される機密保護方法を提供することを目的とする。

【0009】また、この発明は、電子的な取り引きにおいて双方が電子署名を交換し、それを保管することで、この署名データを証拠データとして用いることができるようにするとともに、その署名データの検証を必要に応じて再現できるようにするコンピュータシステムならびに同システムに適用される送受信ログ管理方法および相互認証方法を提供することを目的とする。

【0010】また、この発明は、鍵を管理するデータとして、世代管理番号や有効期限といった情報を付け加えて鍵の世代管理を実現するコンピュータシステムおよび同システムに適用される公開鍵世代管理方法を提供することを目的とする。。

【0011】

【課題を解決するための手段】前述した目的を達成するために、この発明は、公開鍵暗号を用いたワンタイムパスワード方式の相互認証を実行する相互認証機能および前記相互認証を実行し合う相手からの要求に応じてプログラムを起動するサービス機能を有するコンピュータシステムにおいて、前記相手に与える自システム内での権限を決定する識別子を前記相互認証に供される公開鍵と対応づけて格納する識別子格納手段と、前記相互認証の成立を条件に起動される前記相手から要求されたプログラムに対して、その相互認証に供された公開鍵と対応づけられた前記識別子で決定される権限を与える権限付与手段とを具備することを特徴とする。

【0012】この発明においては、他のコンピュータからの要求に応じて起動されるプログラムに対し、他のコンピュータに与える自システム内での権限を適用させることができるため、アプリケーションプログラムの構造に依らずに自システムのセキュリティポリシーを反映させた一貫した機密保護が実行できることになる。

【0013】また、この発明は、転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、送信側および受信側のコンピュータ双方に、前記データ授受の事実を証明するためのログを格納するログファイルと、前記転送データの授受が成立したときに、相手方の電子署名、日時、相手を識別するための識別情報および転送データを識別するための識別情報を含むログを採取して前記ログファイルに記録するログ採取手段とを設けたことを特徴とする。

【0014】この発明においては、データ授受の事実を証明するためのログを採取しておくことにより、データ授受に関して双方の認識に食い違いが発生した場合など、そのログから当該データ授受の事実を調査し証明することが可能となる。

【0015】また、この発明は、転送データに付加される電子署名によって相手の認証およびデータ授受成立の検証を実行するコンピュータシステムにおいて、受信側のコンピュータに、前記転送データを正規に受け入れるときに、その旨を伝えるための受信通知として前記転送データを一意に識別可能な情報を元に生成した電子署名を返送する受信通知手段を設けたことを特徴とする。

【0016】この発明においては、受信通知として署名データを用いることにより、送信者側で受信者の身元確認と正しいデータが受信された旨の確認とを行なえることができるため、受信後の受信者の不正行為やネットワーク上の妨害行為などを防止することが可能となる。

【0017】また、この発明は、第1のコンピュータと第2のコンピュータとの間で公開鍵暗号方式を用いたデータ処理を行なうコンピュータシステムにおいて、前記第1および第2のコンピュータ双方に、それぞれに有効期間が設定された同一人を認証するための複数の公開鍵を前記有効期間に基づいて世代管理する公開鍵世代管理手段を設けたことを特徴とする。

【0018】この発明においては、同一人を認証するための複数の公開鍵を認証側および被認証側の双方で有効期間に基づいて世代管理することにより、たとえば機密保護のために定期的に公開鍵を更新していくような場合に、複数のコンピュータで公開鍵の更新処理の同期が取れるため、タイムラグによる処理のミスを防ぐことが可能となる。

【0019】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

（第1実施形態）まず、この発明の第1実施形態を説明

する。

【００２０】図１には、この第１実施形態に係るコンピュータシステムの構成が示されている。そして、この第１実施形態のコンピュータシステムは、認証機能とシステムのアクセス制御機能との連携にその特徴を有している。

【００２１】ここでは、図１のクライアントプログラム１１からサーバプログラム２１に対して認証要求を出す場合を想定する。このクライアントプログラム１１およびサーバプログラム２１は、それぞれ公開鍵暗号を導入したコンピュータ１０　およびコンピュータ２０　上で動作するものであり、また、コンピュータ１０とコンピュータ２０とは、回線で接続されている。

【００２２】サーバプログラム２１が動作するコンピュータ２０　では、オペレーティングシステム（ＯＳ）によるアクセス制御機能が提供されている。ユーザのプロセスの権限範囲は、そのユーザに割り当てられた識別子ＩＤｘをもとに引き出されるユーザ管理情報に基づいて定められる。そして、この権限情報と各オブジェクト（ファイルやデバイスなどのリソース）に関連づけられたアクセス許可情報とに基づいて、アクセス制御が行なわれる。

【００２３】ここで、この第１実施形態の基本動作について説明する。サーバプログラム２１は、クライアントプログラム１１からの認証要求を受けた際、通信ポートを獲得し、このポートを用いて相互認証処理を行なう。この認証処理は、公開鍵暗号を用いたチャレンジ＆レスポンス方式により行なわれ、公開鍵を用いて相手の身元確認を行なう。

【００２４】この認証が成立すると、サーバプログラム２１は、クライアントプログラム１１の公開鍵に対応づけられた、クライアントプログラム１１のコンピュータ２０上での識別子ＩＤＡを公開鍵ホルダ２２から取り出す。さらに、この識別子ＩＤＡをもとに、クライアントプログラム１１のユーザ管理データをユーザ管理データファイル２３から取り出す。

【００２５】次に、サーバプログラム２１は、クライアントプログラム１１が要求した任意のサービスプログラム２４を起動するが、通常、クライアントプログラム１１から起動されたプログラムは、サーバプログラム２１の権限範囲を継承するので、ここではこれを完全にクリアし、この新たに起動するサービスプログラム２４に対しては、ユーザ管理データで示される権限を新規に設定し直す。さらに、サーバプログラム２１は、クライアントプログラム１１との間に確立された安全な通信ポートをサービスプログラム２４に受け継がせる。

【００２６】このように、権限情報としてシステムの識別子を利用することにより、システムの既存のアクセス制御機能を利用しつつ認証機能を容易に導入でき、かつ、起動されるアプリケーションについても、アクセス制御機能を実装する必要がまったくない。

【００２７】（第２実施形態）次に、この発明の第２実施形態を説明する。図２には、この第２実施形態に係るコンピュータシステムの構成が示されている。そして、この第２実施形態のコンピュータシステムは、データ送受信否認防止のためのログ機能にその特徴を有している。

【００２８】ここでは、図２の送信プログラム３１　から受信プログラム３４　へ転送データＭが送信される場合を想定する。この送信プログラム３１（Ａとする）および受信プログラム３４（Ｂとする）は、それぞれ公開鍵暗号を導入したコンピュータ３０ａおよびコンピュータ３０ｂ上で動作するものであり、また、コンピュータ３０ａとコンピュータ３０ｂとは、回線で接続されている。

【００２９】また、送信プログラム３１および受信プログラム３４は、それぞれ関数（Ａ）と関数（Ｂ）とを呼び出すことで、後述するデータ転送機能を利用することを可能とする。

【００３０】ここで、この第２実施形態の基本動作について説明する。関数（Ａ）は、転送データＭを送信する際に、転送データＭにその時点での日付データＤＡを付加したデータＭ’を作成する。次に、この作成したデータＭ’を一方向性関数により要約した値を鍵ホルダ３２ａに格納されたＡの秘密鍵ＳＫＡによって暗号化して電子署名ＳＩＧＭＡを生成する。そして、データＭ’（電子署名の生成後に暗号化することも可。また、平文Ｍ’のままでも可）に、この電子署名ＳＩＧＭＡを付加したデータを関数（Ｂ）に対して送信する。

【００３１】一方、関数（Ｂ）では、まず、電子署名ＳＩＧＭＡを鍵ホルダ３２ｂに格納されたＡの公開鍵ＰＫＡを用いて復号化する。そして、これと受信したデータＭ’を一方向性関数により要約した値とを比較することにより、送信者の身元確認、受信したデータの正当性（改ざんなどがされていないこと）および電子署名の付加日時を確認する。

【００３２】そして、関数（Ｂ）は、関数（Ａ）に対して受信成功を通知する。受信成功を保証するデータとして、受信データＭ’にその時点での日付データＤＢを付加したデータＭ”を作成し、このデータＭ”を一方向性関数により要約した値をＢの秘密鍵ＳＫＢで暗号化した電子署名ＳＩＧＭＢと日付データＤＢとを送信する。

【００３３】その後、関数（Ａ）は、受信通知ＳＩＧＭＢを鍵ホルダ３２ａに格納されたＢの公開鍵ＰＫＢを用いて復号化する。そして、送信した転送データＭに受信した日付データＤＢを付加したデータＭ”を作成し、この作成したデータＭ”を一方向性関数により要約した値と復号化した受信通知データとを比較することにより、受信者の身元確認、受信されたデータの正当性（明らかにＭが受信されたこと）および受信通知を生成した日付

を確認する。

【0034】そして、関数（A）は、電子署名SIGMBを日付データDBおよび転送データMの転送に関する他の情報とともにログファイル33aに記録するとともに、関数（B）へ受信通知を送信する。一方、関数（B）は、関数（A）からの受信通知を受信すると、電子署名SIGMBと日付データDAとを転送データMの転送に関する他の情報とともに、ログファイル33bに記録する。これにより、データMの送受信が完了する。

【0035】なお、ここでは、受信成功を通知するデータとして、転送データMを一方向性関数により要約した値を用いることとしたが、その代用として転送内容を確実に識別することのできる識別子、すなわち、転送データMを一意に識別できる識別子を用いることも可能である。

【0036】次に、前述した処理の一貫性を保つための機能について説明する。途中でエラーが発生した際には、関数（B）内で完全に受信したデータM'をクリアする。これにより、関数（B）の呼び出しを行なった受信プログラム34は、転送データMを得る術がなくなる。

【0037】また、ログファイル33aまたはログファイル33bへの記録後にエラーが発生した場合には、ログの内容を更新し、データ転送がエラー終了したことを必ず記録する。これにより、実際のデータ転送の事実とログへの記録内容とに食い違いが発生することがなくなる。

【0038】なお、ログファイル33aおよびログファイル33bには、少なくとも以下の情報が記録される。

（1）署名データSIGMX（X：AまたはB）。

（2）日付データDX（X：AまたはB）。

（3）通信相手X（X：AまたはB）を識別する情報。具体的には、正しい公開鍵PKX（X：AまたはB）を得ることができる情報。

（4）転送データMを識別する情報。具体的には、転送データMを復元することができる情報。

【0039】これらの情報は、以下のいずれかの方法で記録される。

（1）ログファイル内に転送データMを保存する。

（2）別ファイルにMを保存する。ログファイル内にはMの識別子を記録し、識別子から転送データMを取り出せるようにする。

（3）転送データMは分解された状態で、データベースなど、各種の方法で管理される。ログファイル内には、Mの識別子を記録し、識別子をもとに、各ファイルデータベースなどで管理されているデータを引き出し、これらを用いて転送データMを組み立てる。

【0040】次に、図3を参照して、他のコンピュータとの間のデータ授受について検証を行なう場合を説明する。ここでは、図3のコンピュータ40と他のコンピュータ（Xとする）との間のデータ授受に関するログが、前述したいずれかの方法で採取されているものとする。また、鍵ホルダ42には、電子署名作成時の鍵が保持されているものとする。

【0041】検証プログラム41は、まず、ログファイル43から得られた転送データ識別情報より、検証の対象となる電子署名データに対応する転送データMの転送時のイメージを以下のいずれかの方法で復元する。

（1）ログファイル43内に保存されたデータMを読み出す。

（2）識別子から別ファイルに保存されたデータMを読み出す。

（3）識別子からデータベース44上のデータを引き出し、これらを用いてデータMを組み立てる。

【0042】次に、検証プログラム41は、ログファイル43より、日付データDXを取り出して、データMにDXを付加したデータMを生成する。そして、このデータMのハッシュ値を計算する。

【0043】また、検証プログラム41は、ログファイル43より、電子署名データSIGMXと通信相手の情報Xを取り出す。そして、この情報Xをもとに、鍵ホルダーから公開鍵PKXを取り出し、SIGMXをPKXにて復号化する。

【0044】そして、先程計算したデータMのハッシュ値とSIGMXをPKXにて復号化した値と値が一致した場合、検証プログラム41は、データMの送受信がコンピュータ40と他のコンピュータとの間で行なわれたこと、正しい相手と正常な転送処理が行なわれたこと、および通信相手が日付DXの時点で転送の事実を承認していることを確信する。

【0045】このように、転送データ、電子署名および日付データなどを保持することによって、データ授受に関して双方の認識に食い違いが発生した場合など、ログファイルに記録された情報から行なわれたデータ授受の事実を調査することが可能となる。また、転送データを復元して電子署名の検証を再現することが可能となるため、電子署名を取引の証拠として用いることができる。

【0046】（第3実施形態）次に、この発明の第3実施形態を説明する。図4には、この第3実施形態に係る鍵ホルダの形式が示されている。そして、この第3実施形態では、公開鍵暗号における鍵世代管理にその特徴を有している。

【0047】ここでは、暗号化および復号化に用いる鍵を管理するための鍵ホルダに、各鍵ごとに少なくとも以下の情報が含まれるものとする。

（1）鍵データ。

（2）鍵の所有者名。

（3）世代管理番号。

（4）有効期限。

（5）世代管理番号。この世代管理番号は、鍵の使用ま

たは未使用、および鍵の使用順序を識別可能な値が設定される。ここでは、仮に世代管理番号の設定内容を以下のように定める。

0：新規の鍵（未使用）
1：カレントで使用中の鍵
2～：変更済みの鍵
（6）有効期限。

【0048】以下に、このような鍵情報を用いた鍵の自動更新処理および検証処理の例を挙げる。

（自動更新処理）鍵サーバは、配布する鍵の世代管理番号を0に設定する。また、適当な有効期限を設定して配布する。なお、鍵サーバを設置して鍵を配布する場合の他、ローカルで鍵を生成する場合も考えられるが、この場合も設定内容は同様である。また、公開鍵は配布の必要があるので、これについても、鍵サーバを設置する場合、しない場合とも同様に、前述のような設定を行なった上で配布を行なう。そして、公開鍵および秘密鍵とも同様に管理する。

【0049】鍵を配布された側は、新規の鍵を鍵ホルダへ登録する。この際、世代管理番号および有効期限は、配布した側で設定した値を保持している。ここでは、図4内の（C）を登録したとする。

【0050】ここで、新規の鍵の鍵情報に含まれる有効期限情報をカレントの鍵の有効期限が切れるタイミングとする。この時点で、鍵の変更が発生する。このとき、同一の所有者名を持つ鍵のすべての世代管理番号をインクリメントする。たとえば、図4においては、1997年12月5日の0時0分0秒のタイミングで鍵が更新され、（A）、（B）および（C）の各鍵の世代管理番号がインクリメントの対象となる。そして、図5は、更新処理を行なった後の鍵ホルダ内のイメージを示す図である。

【0051】これにより、世代管理番号0であった新しい鍵がカレントの鍵となる。図5においては、（C）の鍵が新しい鍵として使用される。

（暗号化または復号化のための鍵取り出し処理）暗号化または復号化のために鍵を取り出す場合には、所有者名情報と世代管理番号とに基づいて鍵を検索する。

【0052】たとえば、図4においては、ユーザAAAAのカレントで暗号化・復号化に用いる鍵は（B）の鍵が用いられる。また、システム間の時計の差を考慮し、有効期限に対して誤差の許容範囲を定めておく。すなわち、カレントの鍵で復号化できない場合であって、前述の許容範囲内に収まる時間である場合は、世代管理番号0の鍵で復号化を試みてみる。同様に、鍵の変更後、カレントの鍵で復号化できず、許容範囲内に収まる時間である場合は、世代管理番号2の鍵で復号化を試みる。

【0053】（検証のための鍵取り出し処理）検証のために鍵を取り出す場合には、鍵の所有者名と電子署名を生成した日付データとを用いて、検証の対象となる電子署名を生成した鍵を検索する。具体的には、鍵ホルダに保持されている各鍵の有効期限と世代管理番号とを用いることによって、鍵の使用期間を特定することができる。これにより、正しい鍵を検索することが可能となる。

【0054】このように、鍵の自動更新を行なうことにより、複数のコンピュータ間で鍵登録の同期をとることができ、また、誤差許容範囲を定めることによって、タイムラグによる処理のミスを減少させることができる。

【0055】

【発明の効果】以上詳述したように、この発明によれば、他のコンピュータからの要求を受けて自システムで起動するプログラムに対して、システムのアクセス制御を適用させることができるため、アプリケーションプログラムの構造に依らず、システムのセキュリティポリシーが反映され、一貫した管理が可能となる。

【0056】また、権限情報としてシステムの識別子を利用することにより、システムの既存のアクセス制御機能が利用できるため、認証機能の導入が容易であり、起動されるアプリケーションにアクセス制御機能を実装する必要がないため、アプリケーションプログラムの開発が容易になる。

【0057】また、権限情報としてシステムの識別子を利用することにより、システムの既存のユーザ管理機能と公開鍵暗号を用いたセキュリティ機能とを連携させて利用することが可能となるため、新しいセキュリティ機能の導入が容易になり、関連するアプリケーションプログラムの開発が容易になる。

【0058】また、データ授受に関するログを保持することにより、双方の認識に食い違いが発生した場合に、ログに記録された情報から、行なわれたデータ授受の内容を調査することが可能となる。また、転送データを復元して電子署名データの検証を再現することが可能となり、電子署名データを取引の証拠として用いることができる。さらに、送受信とログの内容との整合性を確保するので、エラーによる不整合を防ぐことができる。

【0059】また、受信通知として署名データを用いることにより、送信者側で受信者の身元確認および正しいデータが受信されたことの確認が得られるため、受信後の受信者の不正行為やネットワーク上の妨害行為などを防ぐことができる。

【0060】また、日付情報を含めたデータの電子署名を作成することにより、送信者の身元確認とデータの保全性とともに電子署名鍵印の日付も保証されるため、証拠としての電子署名の利用が可能となる。

【0061】また、鍵の世代管理を自動的に行なうことにより、複数のコンピュータ間で鍵登録の同期がとれ、また、それぞれのコンピュータの時計の差により発生するタイムラグによる処理ミスを誤差許容範囲を定めることによって減少させることが可能となる。また、従来使

い捨てであった鍵を系統だって管理することにより、正しい検証が可能になる。

【図面の簡単な説明】

【図1】この発明の第1実施形態に係るコンピュータシステムの構成を示す図。

【図2】同第2実施形態に係るコンピュータシステムの構成を示す図。

【図3】同第2実施形態の他のコンピュータとの間のデータ授受について検証を行なう場合を説明するための図。

【図4】同第3実施形態に係る鍵ホルダを示す図。

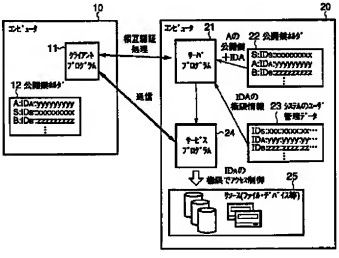
【図5】図4の鍵ホルダに対して更新処理を施した後の状態を示す図。

＊【図6】第3者による送信者のなりすましやネットワーク上でのデータの改ざんまたは破壊などを示す図。

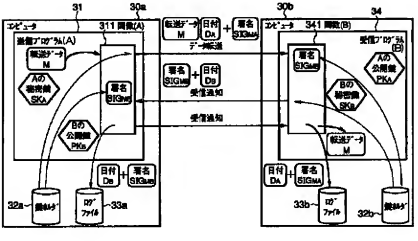
【符号の説明】

10…コンピュータ、11…クライアントプログラム、12…公開鍵ホルダ、20…コンピュータ、21…サーバプログラム、22…公開鍵ホルダ、23…ユーザ管理データファイル、24…サービスプログラム、25…リソース、30a，30b…コンピュータ、31…送信プログラム、32a，32b…鍵ホルダ、33a，33b…ログファイル、40…コンピュータ、41…検証プログラム、42…鍵ホルダ、43…ログファイル、44…データベース。

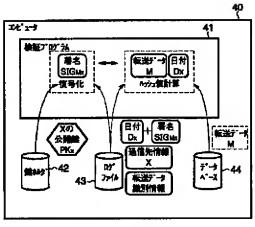
【図1】



【図2】



【図３】



【図４】

登録日付：所有者名：鍵ﾃﾞｰﾀ：世代管理番号：有効期限：・・・	
1997/01/1：AAAA：xxxxxxxxxxxx：3：1997/01/5/0:00:00：……(A)	
1997/05/1：CCCC：xxxxxxxxxxxx：1：1997/05/5/0:00:00：……	
1997/05/1：BBBB：xxxxxxxxxxxx：1：1997/05/5/0:00:00：……	
1997/06/1：AAAA：xxxxxxxxxxxx：1：1997/05/5/0:00:00：……(B)	
1997/12/1：AAAA：xxxxxxxxxxxx：0：1997/12/5/0:00:00：……(C)	
1997/12/1：BBBB：xxxxxxxxxxxx：0：1997/12/5/0:00:00：……	

【図５】

登録日付：所有者名：鍵ﾃﾞｰﾀ：世代管理番号：有効期限：・・・	
1997/01/1：AAAA：xxxxxxxxxxxx：3：1997/01/5/0:00:00：……(A)	
1997/05/1：CCCC：xxxxxxxxxxxx：1：1997/05/5/0:00:00：……	
1997/05/1：BBBB：xxxxxxxxxxxx：1：1997/05/5/0:00:00：……	
1997/06/1：AAAA：xxxxxxxxxxxx：2：1997/06/5/0:00:00：……(B)	
1997/12/1：AAAA：xxxxxxxxxxxx：1：1997/12/5/0:00:00：……(C)	
1997/12/1：BBBB：xxxxxxxxxxxx：0：1997/12/5/0:00:00：……	

【図６】